



# November 2007





## How Do You Choose Good Passwords?

Most people use a password that is based on personal information because it is easy to remember. That also makes it easier for an attacker to guess it. Is your's a combination of the month, day or year of your birthday; the last four digits of your social security number; address or phone number? Consider how easy it is to find out this information. Is it a word that can be found in the dictionary? If so, it is susceptible to attacks which attempt to guess passwords using words in the dictionary.

Although intentionally misspelling a

word ("daytt" instead of "date") may offer some protection against "dictionary" attacks, an even better method is to use letters from a phrase and rely on a memory technique (mnemonic) to help you decode it. For example, instead of the password "hoops," use "ILtpBb" for "[I] [L]ike [t]o [p]lay [B]asket[b]all." Using both upper and lowercase letters adds an additional layer of protection.

Your best defense is to use a combination of numbers, special characters and both upper and lowercase letters. Change the example above to "IL2pBb!" and see how much more complicated it becomes. After developing a strong password, don't use it for every system or program you log in to. If an attacker guesses it, access would be available to all your accounts. Use these techniques to develop unique passwords for each of your accounts.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10 
11 Veterans Day 	12 Veterans Day Holiday	13	14	15	16	17
18	19	20	21	22  Thanks-giving Day	23 	24
25	26	27	28	29	30	



ADOA Information Security

**AIS**

Managing Our Information Safeguards

Phone: 602•542•2252

E-mail: [adoa.infosec@azdoa.gov](mailto:adoa.infosec@azdoa.gov)

<http://www.azdoa.gov/isd/ais>